

FIG. 1 (PRIOR ART)

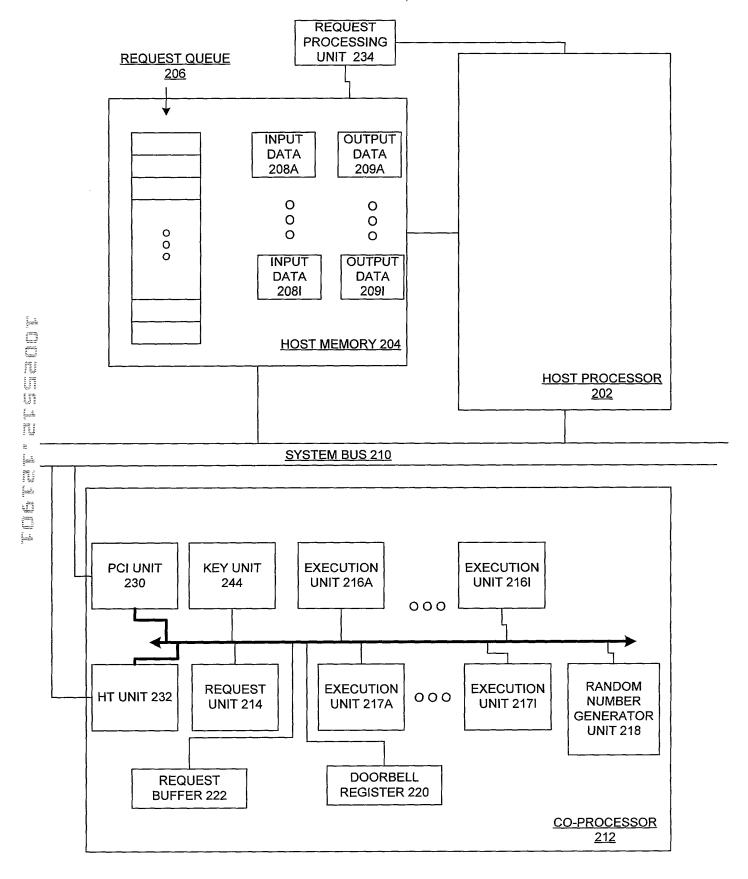


FIG. 2

OPERATION CODE 302	SIZE 304	PARAMETERS 306	DATA LENGTH 308
	à	DATA POINTER 310	
	RE	RESULT POINTER 312	

REQUEST FORMAT 300

FIG.

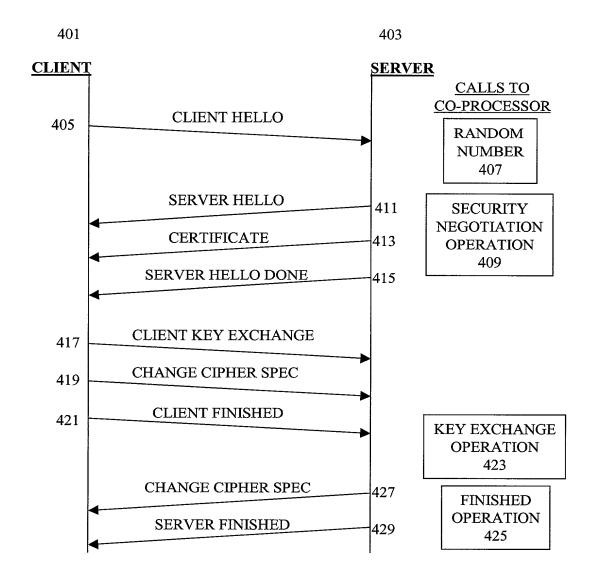


FIG. 4

MACRO SECURITY OPERATIONS	PRIMITIVE SECURITY OPERATIONS
SECURITY NEGOTIATION OPERATION	2 partial hash OPERATIONS (1 MD5 and 1 SHA1)
KEY EXCHANGE OPERATION	1 - RSA OPERATION 20 Hash OPERATIONS (10 MD5 + 10 SHA1) for SSL 3.0
	76 Hash OPERATIONS (40 MD5 + 36 SHA1) for SSL 3.1 2 partial hash OPERATIONS (1 MD5 and 1 SHA1)
FINISHED OPERATION	1 - decrypt OPERATION (RC4 or 3DES or DES or AES) 2 - hash OPERATIONS for MAC (either MD5 or SHA1) 4 - hash OPERATIONS (2 MD5 + 2 SHA1) 4 - hash OPERATIONS (2 MD5 + 2 SHA1) 1 - encrypt OPERATION (RC4 or 3DES or DES or AES) 2 - hash OPERATIONS for MAC (either MD5 or SHA1)

FIG. 5

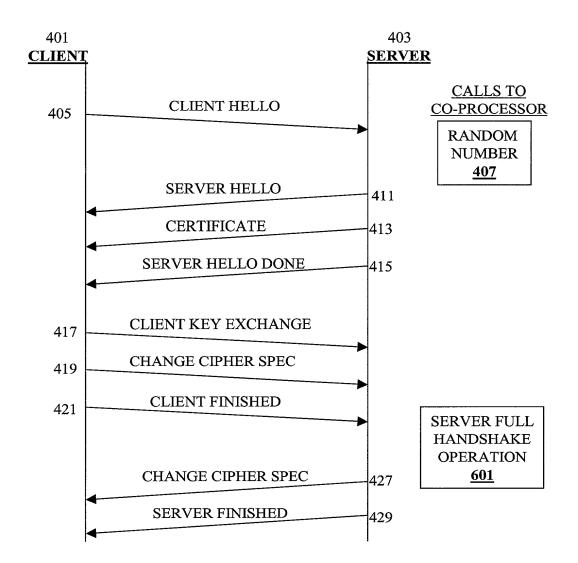


FIG. 6

MACRO SECURITY OPERATION	PRIMITIVE SECURITY OPERATIONS
FULL HANDSHAKE OPERATION	1 - RSA OPERATION 20 Hash OPERATIONS (10 MD5 + 10 SHA1) for SSL 3.0
	76 Hash OPERATIONS (40 MD5 + 36 SHA1) for SSL 3.1
	6 – hash OPERATIONS (3 MD5 + 3 SHA1)
	1 – encrypt OPERATION ((A)RC4 or 3DES or DES or AES)
	6 – hash OPERATIONS (3 MD5 + 3 SHA1)
	1 - encrypt OPERATIONS ((A)RC4 or 3DES or DES or AES)
	2 – hash OPERATIONS for MAC (either MD5 or SHA1)

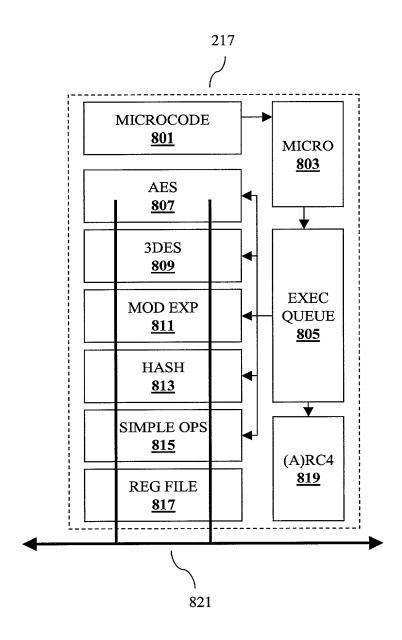


FIG. 8

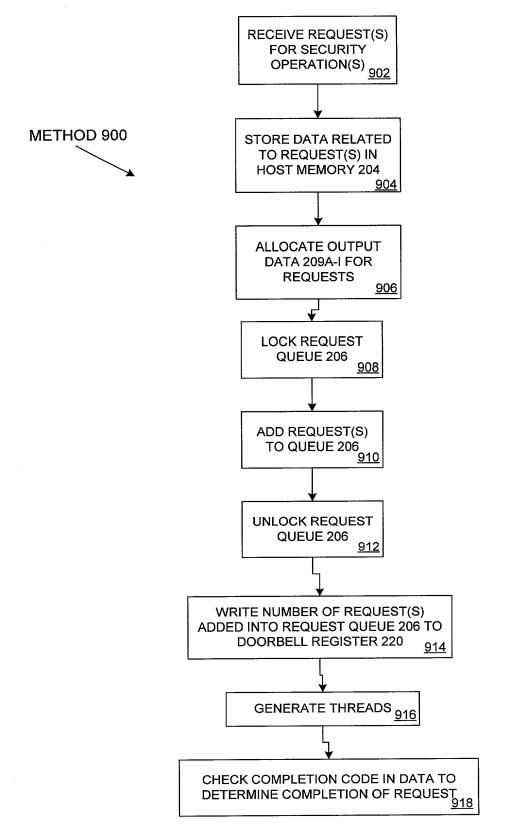


FIG. 9

005655.P003 "An Interface For a Security Coprocessor" Richard E. Kessler, et al.

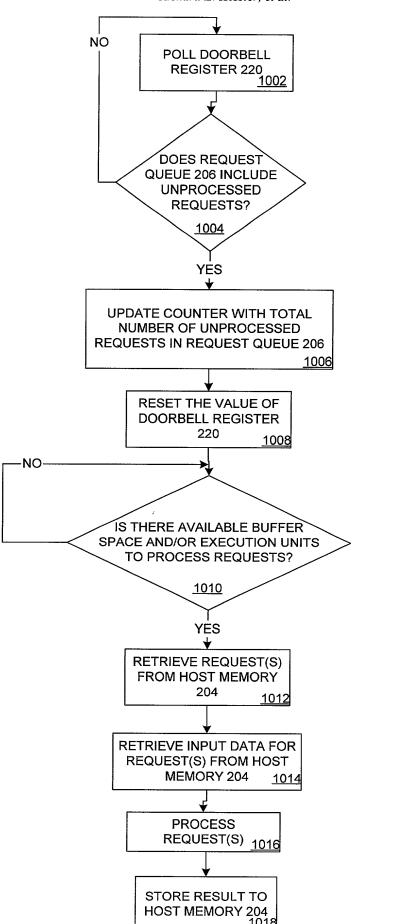


FIG. 10